IN THE CLAIMS:

Please amend the claims as follows.

1. (Canceled)

2. (Currently Amended) ~~A~~ The method as claimed in claim ~~1~~ 30, in which the information encrypted by the recording encryption key (E (NE)) comprises control word information (CW) usable to descramble a scrambled data transmission also recorded on the support medium.

3. (Canceled)

4. (Currently Amended) ~~A~~ The method as claimed in claim ~~1~~ 30, in which the transmitted information is encrypted prior to transmission and received by a decoder means before being communicated to the recording means.

5. (Currently Amended) ~~A~~ The method as claimed in claim 4, in which the decoder is associated with a portable security module used to store transmission access control keys (KO(NS), KO'(Op1, NS) etc.) used to decrypt the transmitted encrypted information.

6. (Currently Amended) ~~A~~ The method as claimed in claim 5, in which at least one of the recording encryption key (E (NE)) and/~~or~~ the recording transport key (RT (A)) function in accordance with a first encryption algorithm (DES) and the transmission

access control keys (KO(NS), KO' (Opl, NS) etc.) function in accordance with a second encryption algorithm (CA).

7. (Currently Amended) ~~A~~ The method as claimed in claim ~~1~~ 30, which the recording transport key (RT (A)) is generated at a central recording authorization unit and a copy of this key communicated to the recording means.

8. (Currently Amended) ~~A~~ The method as claimed in claim 7, in which the recording transport key (RT (A)) is ~~preferably~~ encrypted by a further encryption key (KO(NSIM)) prior to being communicated to the recording means.

9. (Currently Amended) ~~A~~ The method as claimed in claim ~~1~~ 30, in which a central access control system communicates transmission access control keys (KO (NS), KO'(Op1, NS) etc.) to the recording means.

10. (Currently Amended) ~~A~~ The method as claimed in claim 9, in which the transmission access control keys (KO(NS), KO' (Opl, NS) etc.) are communicated to a portable security module associated with the recording means.

11. (Currently Amended) ~~A~~ The method as claimed in claim 9, in which the recording means directly descrambles transmitted information using the transmission access keys (KO (NS), KO'(Op1, NS) etc.) prior to re-encryption of the information by the recording encryption key (E (NE)) and storage on the support medium.

12. (Currently Amended) ~~A~~ The method as claimed in claim 9, in which the central access control system ~~preferably~~ encrypts the broadcast access control keys (KO(NS), KO' (Op1, NS) etc.) by a further encryption key (KO (NSIM)) prior to their communication to the recording means.

13. (Currently Amended) ~~A~~ The method as claimed in claim 9, in which the recording means sends a request to the central access control system including information identifying the broadcast access keys needed (KO(NS), KO'(Op1, NS) etc.), the request of authentification by the recording means using a key (KO(NSIM)) unique to that recording means.

14. (Currently Amended) ~~A~~ The method as claimed in claim ~~1~~ 30, using a decoder means and associated security module and a recording means and associated security module and in which a copy of the recording transport key (RT (A)) is stored in at least one of the security module associated with the decoder means and~~/or~~ the security module associated with the recording means.

15. (Currently Amended) ~~A~~ The method as claimed in claim 14, in which the recording transport key (RT (A)) is generated by either the recording security module or decoder security module and communicated to the other security module.

16. (Currently Amended) ~~A~~ The method as claimed in claim 15, in which the

recording transport key (RT (A)) is ~~preferably~~ encrypted before communication to the other security module and decrypted by a key unique (KO(NS)) to that other security module.

17. (Currently Amended) ~~A~~ The method as claimed in claim 16, in which the decoder security module and recording security module carry out a mutual authorization process, the unique decryption key (KO (NS)) being passed to the other security module from the encrypting security module depending on the results of the mutual authorization.

18. (Currently Amended) ~~A~~ The method as claimed in claim 17, in which the mutual authorization step is carried out using, inter alia, an audience key Kl (C) known to both security modules.

19. (Currently Amended) ~~A~~ The method as claimed in claim 14, in which the decoder security module possesses transmission access control keys (KO(NS), KO' (Op1, NS) etc.) to decrypt the transmitted information in an encrypted form and a session key (K3 (NSIM)) re-encrypt the information prior to communication to the recording security module, the recording security module possessing an equivalent of the session key (K3 (NSIM)) to decrypt the information prior to encryption by the recording transport key (RT (A)).

20. (Currently Amended) ~~A~~ The method as claimed in claim 19, in which the session key (K3 (NSIM)) is generated by one of the decoder security module ~~or~~ and recording

means security module and communicated to the other module in encrypted form using an encryption key (KO (NS)) uniquely decryptable by other security module.

21.-29. (Cancelled)

30. (New) A method of recording transmitted digital data, comprising:

encrypting transmitted digital information of the transmitted digital data by a recording encryption key;

storing the encrypted, transmitted digital information by a recording means on a recording support medium;

encrypting an equivalent of the recording encryption key by a recording transport key;

storing the equivalent of the recording encryption key to the support medium together with the encrypted information, wherein at least one of the encryption key and recording transport key is stored on a portable security module associated with the recording means.

31. (New) A system for recording transmitted digital data, which is encrypted by a recording encryption key, comprising:

a receiver/decoder for at least receiving the encrypted, transmitted digital data; and

a recording means for recording the encrypted, transmitted digital data to a recording support medium, along with an equivalent of the recording encryption key, wherein the equivalent recording encryption key is encrypted via a recording transport key and stored with the recording means.

32. (New) The system as claimed in claim 31, further comprising:

a decoder means and associated security module adapted to store a copy of the recording transport key (RT(A)).

33. (New) The system as claimed in claim 32, in which the security module associated with the decoder means is adapted to descramble transmitted information using one or more transmission access keys prior to re-encryption by a session key for subsequent communication to the recording means.